Demonstration of Quantum Algorithms and Quantum Computing Hardware

Task Leader & Research Team

Dr. Colin P. Williams, Quantum Algorithms & Technologies Group, Section 365, JPL
email: Colin.P.Williams@jpl.nasa.gov, tel: (818) 393 5352
Dr. Daniel Abrams, (JPL, Quantum Algorithms & Technologies Group)
Dr. Nicolas Cerf (Free University of Brussels)
Dr. Julia Dunphy (Contractor, Java/C++ programming)
Dr. Pierre Echternach, (JPL, Microdevices Laboratory)
Dr. James Franson, (no-fee collaborator, APL, Johns Hopkins University)

Product Description

Many computational problems of relevance to the Space Sciences Enterprise, such as planning, scheduling, and spacecraft design and others related to the Earth Sciences Enterprise, such as data analysis and high bandwidth communications, are currently regarded as intractable. That is, the computational cost of solving the problems grows exponentially with the size of the problem. Nevertheless NASA has no choice but to attempt to solve such problems. Current approaches rely upon sophisticated computer science techniques, and high performance hardware. While these approaches can be implemented today they do not truly *beat* intractability but do delay its onset to slightly larger cases.

We are pursuing a more fundamental attack on intractability by developing quantum computers to solve problems traditionally regarded as being intractable. Our goal is to extend the range of computational problems known to be solvable in ideally exponentially, but more likely polynomially, fewer steps on a quantum computer than on a classical computer. We are also building prototype quantum computer hardware based on solid state quantum electronics (at JPL) and quantum optics (at APL).

The products of our research fall into three categories. (1) Technical papers describing new quantum algorithms, (2) Software tools for designing quantum circuits that implement those algorithms and (3) Designs for scalable quantum computer architectures that will be able to implement our quantum algorithms. Our proposal is therefore for a balanced research program in quantum computing that leverages NASA and non-NASA sources of funding and which will lead ultimately to quantum computing hardware and software. This is a **continuing**, **push** task.

Benefits

- Quantum algorithms can solve some computational problems in *exponentially* (and many more in *polynomially*) fewer steps than required using any conventional classical computer – even a supercomputer. This is not technological (faster chip) advantage but a fundamental computational complexity (fewer steps) advantage, unmatchable by *any* classical computer.
- Quantum computers can perform computational *tasks* that *no* classical computer can do such as teleporting information [Ben94], communicating with messages that betray eavesdropping and simulating physical systems beyond the reach of classical computers [Abr98].
- The benefit of the quantum approach can be quantified by comparing the computational complexities of the quantum algorithm against the best classical counterpart. Our quantum algorithm for NP-hard problems has a complexity that is the *cube root* of that of a naïve classical algorithm and roughly *equal to* that of the *best* known classical tree search algorithm for solving such problems [Pat98]. In FY'00 we plan to improve upon our existing algorithm and invent others.

- The benefit of having theorists team with experimentalists is that we have discovered new quantum gates that appear to be easier to implement (as judged by the experimentalists) than the "standard" quantum gates (controlled-NOT) used by others. This makes quantum computing more feasible.
- Breakthroughs in quantum computer hardware and algorithm design lead to patents and intellectual property assets of measurable dollar value to JPL. We have filed a patent on a new quantum technology derived from our work and have spun-off a start-up company to commercialize it.

Technical Approach

- Our approach harnesses quantum effects such as superposition, interference, entanglement, non-locality, non-determinism and non-clonability to solve problems vastly more efficiently than is possible using a classical computer. These physical effects are not available to a classical computer.
- We pursue a three-pronged research program that addresses
  (1) the discovery of new quantum algorithms,
  (2) the design of circuits that implement those algorithms and
  (3) the design of hardware for the actual quantum computer.
- In **this** proposal we emphasize quantum algorithms work as our quantum hardware efforts receive partial funding from other sources. Nevertheless, overall we balance hardware and algorithms.
- Our quantum computing research is integrated with parallel development of quantum sensors such as
  (1) a quantum optical gyroscope,
  (2) a quantum gravity gradiometer and
  (3) a quantum gravity wave detector.

  The improvement in sensitivity provided by the quantum sensors is between **one million** and **one hundred million** times above the current state of the art.

The quantum sensor research and quantum computer research are intimately related due to an isomorphism between quantum interferometry (on which the quantum sensors are based) and quantum circuit theory (on which the quantum computers are based). Knowledge gained from funding the quantum algorithms work carries over to our quantum sensors work and vice versa. This isomorphism has allowed us to take concepts from fault-tolerant quantum computing and apply them to our quantum optical gyroscope, thereby making a better gyroscope overall. We expect our quantum sensors to be flight-ready within a decade and the knowledge gained to catalyze the development of quantum computing hardware.

Quantum Algorithms

Our technical approach to developing new quantum algorithms is to express a desired computation in terms of a **sequence of elementary unitary operators**. Some computations, e.g., the discrete Fourier transform, are easily couched this way because they happen to be unitary to begin with. However, the more interesting computations, such as *k*-SAT, are non-unitary making their conversion to quantum computing more challenging [Hog96, **Cer98**].

There are already several quantum algorithms whose performances surpass those of conventional (classical) algorithms. Shor's quantum algorithm for factoring composite integers [Sho94], the Deutsch-Jozsa algorithm for deciding whether a function is constant or balanced [Cle97] and the Abrams-Lloyd algorithm for simulating quantum physics [Abr98], all run *exponentially* faster than the best known classical counterparts. Similarly, Grover's algorithm for unstructured quantum search [Gro96], the Cerf-Grover-Williams algorithm for nested quantum search for solving NP-hard problems (including, for example, scheduling, planning, constraint

satisfaction, design, diagnosis) [**Cer98**], and the Abrams-Williams algorithm for Monte Carlo integration [**Abr99**], all offer a *polynomial* speedup with respect to their classical counterparts.

In FY'00 we plan on building upon our successes of our structured quantum search [**Cer98**], parallel quantum search [**Gin99**] and quantum wavelet transforms [**Fij99**] by developing new quantum analogs of classical randomized algorithms and techniques for quantum data compression. This will build upon work reported by Hogg [Hog98] and Selman [Sel92].

Quantum Circuit Design

Having devised a quantum algorithm, the next step toward implementing it is to design a compact quantum circuit that encodes the algorithm. This is a highly non-trivial process. In FY'99 our (successful) technical approach to this problem was to invent a genetic algorithm for quantum circuit design [**Wil99**]. In FY'00 we plan on extending this approach to include algebraic [Tuc99] and numerical methods [DiV94]. A good starting point is Robert Tucci's Qubiter computer program [Tuc99]. This tool is in its infancy and has no user friendly interface and while it uses one of the best algorithms available, is still not capable of producing very optimal circuits. We propose to take Qubiter and our genetic algorithm as starting points and build an integrated quantum circuit design tool that produces more compact quantum circuits that implement quantum algorithms of interest. The tasks include:

1. Adding a JNI interface to the VC++ code in which Qubiter is written.
2. Writing a user interface in Java which allows the user to observe the circuits produced by the matrix reduction in graphical form and make manual improvements to the circuits calculated
3. Write a program that can verify that the user entered optimizations are valid with respect to the original matrix.
4. Develop a metric for the goodness of the circuit generated by the tool (e.g. number of elementary operations)
5. Integrate the algebraic approach with the genetic algorithm tool we have developed.

Quantum Computing Hardware

Although the main effort in this proposal is in quantum algorithms, the algorithms work helps to motivate and guide the fabrication of solid state and optical quantum hardware. One of the obstacles to practical quantum computers has been the inability to devise a *scalable* architecture. For example, single ions and photons interacting with single atoms in optical microcavities have been used. These systems are not easily integrated into larger devices. In the last two years there have been two major breakthroughs, which have changed this picture. With support from extensive theoretical calculations, it was suggested by a German group [Shn97, Mak99] that superconducting Coulomb blockade devices would be very well suited as qubits; the basic building block for quantum computers. The Coulomb blockade devices have the very important advantage that they can be integrated easily into larger systems, since they are based on existing microelectronics fabrication technology, which is very well advanced. These systems are macroscopic and can offer a macroscopically coherent quantum state from superconductivity. Until six months ago this concept was only theoretical, since quantum coherence had never been observed in this kind of macroscopic system. In a ground-breaking experiment, a Japanese group from NEC demonstrated macroscopic quantum coherence in a so-called single Cooper-pair box. This result was published in *Nature* in late April of this year [Nak99]. The combination of these two very important results shows that it would be possible to implement the basic qubit operations in a Coulomb-blockade-based device. We have already fabricated such a device. The decoherence time of a single qubit has been measured to be greater than nanoseconds, but the theory predicts a lifetime of milliseconds. With gate switching rates of picoseconds, this gives us the potential for tens of thousands of operations per coherence time. A photograph of our solid state qubit is shown below. This device is not intended to be a particularly useful computer in its own right, but rather to serve as a development vehicle for the first true "quantum transistor", the essential building block on the road to scalable quantum computer hardware.

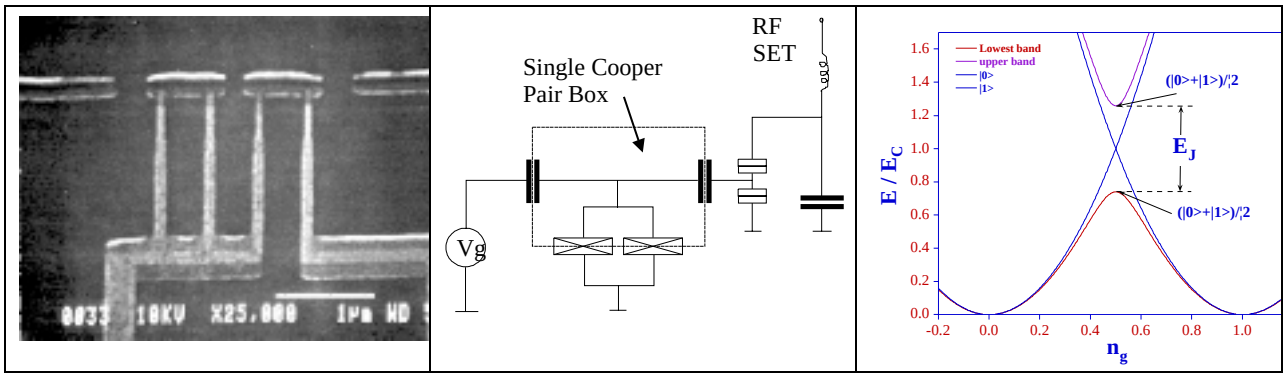
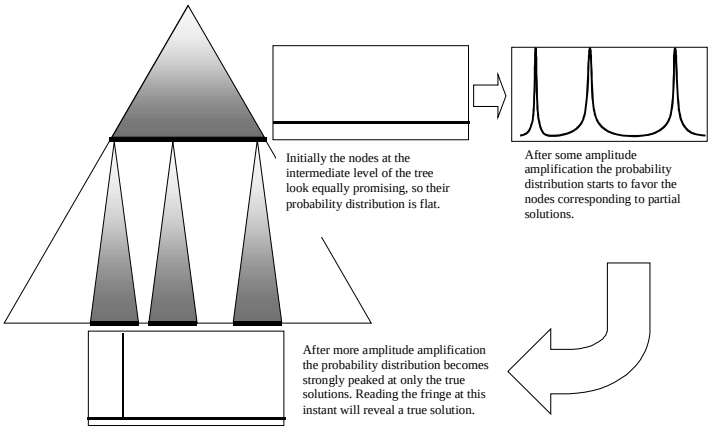


Fig. 1 JPL single Cooper-pair box in close proximity to a single electron transistor (left); schematic of SCP box and SET readout. (center); and level diagram of SCP box (right).

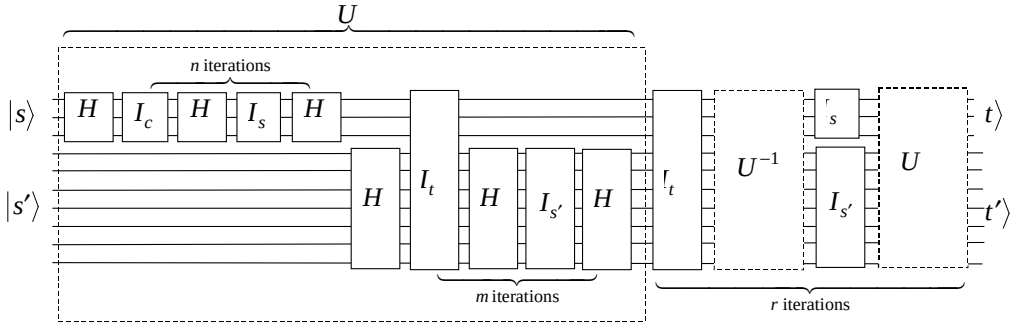
Status and Milestones

This is a **continuing** task. In the first year of the project, we accomplished the following:

1. Nicolas Cerf, Lov Grover and Colin Williams invented a quantum algorithm for solving structured search problems [**Cer98**]. This is currently the best know quantum algorithm for solving NP-hard problems and has a complexity comparable to the best classical tree-search algorithm [Pat98]. Our complexity is still exponential, but with a smaller exponent than that of a naïve tree search algorithm.

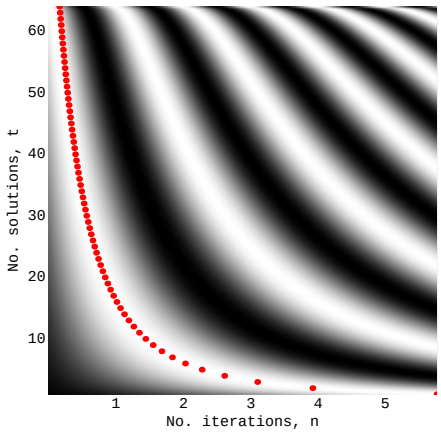


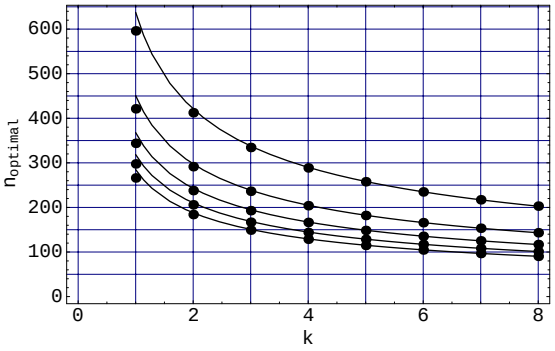
2. We devised the following circuit implementation of our structured search algorithm [**Cer98**].



3. Gingrich, Williams and Cerf invented a generalized parallel quantum search algorithm [**Gin99**]. The figure shows the probability of success of our search algorithm as a function of the number of solutions and the number of amplitude amplification operations (white =

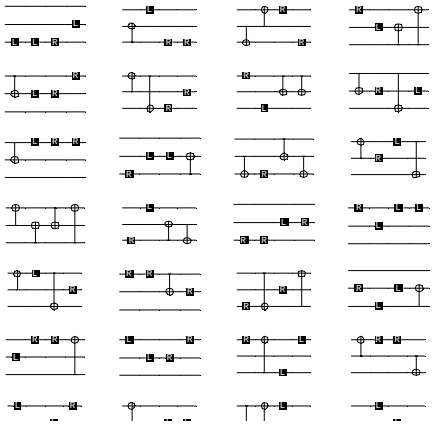
probability 1, black = probability 0). On the right we show how the optimal number of amplitude amplification operations varies with the degree of parallelism. The solid curve is our theoretical prediction and the data points are from numerical simulations of parallel quantum search.

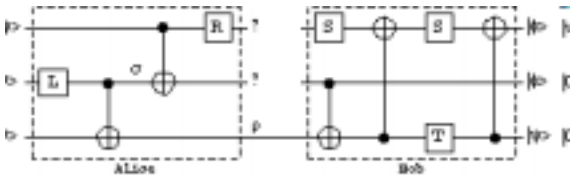




4. Fijany and Williams invented quantum algorithms and quantum circuit implementations of various discrete quantum wavelet transforms [**Fij99**]. The quantum wavelet transform can be used in quantum data compression and quantum signal processing.

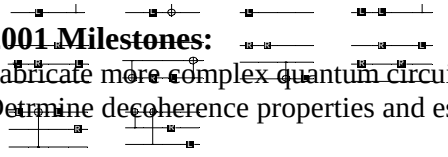
5. Gray and Williams wrote a genetic algorithm for performing automated quantum circuit design [Wil99]. The algorithm found a better (more compact) teleportation circuit than that known at the time. On the left below we see part of a population of random circuits. On the right we see the quantum teleportation circuit that our algorithm improved upon.





FY 2000 Milestones:

1. Develop quantum analogs of classical randomized algorithms such as GSAT [Sel92] and Walk-SAT.
2. Exhibit novel data compression algorithm based on our quantum wavelet transform.
3. 3Improve designs for scalable quantum computer hardware in collaboration with the JPL Microdevices Laboratory (for quantum electronics) and the Applied Physics Laboratory at Johns Hopkins University (for quantum optics).
4. Perform a rational reconstruction/enhancement of our quantum circuit design tool.



FY 2001 Milestones:

1. Fabricate more complex quantum circuits.
2. Determine decoherence properties and estimate scalability.

3. Build simulators for both JPL solid state quantum computing scheme and APL optical scheme.
4. Determine minimum size example of one of our quantum algorithms to run on our hardware.

FY 2002 Milestones:

1. Demonstrate running a rudimentary quantum algorithm in hardware.
2. Refine quantum algorithms.
3. Consider higher level quantum computer architectures e.g., quantum cellular automata.

Customer Relevance

This project provides a general advance in computer technology that could be applicable across Space Sciences, Earth Sciences and Aeronautics Enterprises. Specifically, it could be used by Space Sciences Enterprise for spacecraft design, mission planning, and dynamically fast re-planning of observations during a time-critical fly-by. The technology could also be used by the Earth Sciences Enterprise for advanced data analysis. Dr. Leon Alkalai, the Head of the Center for Integrated Space Microsystems has expressed interest in using our quantum computing technology and has written a letter of support. We could potentially collaborate with Dr. Deepak Srivastava at NASA Ames who has been funded for "Prototyping of Solid-State Quantum Computers: A Pathway for Revolutionary Computing".

Technical References

[Abr98] D. S. Abrams and S. Lloyd, "A Quantum Algorithm Providing Exponential Speed Increase for Finding Eigenvalues and Eigenvectors," Available as Los Alamos preprint http://xxx.lanl.gov/abs/quant-ph/9807070 (1998)

[Abr99] D. S. Abrams and C. P. Williams, "Fast Quantum Algorithms for Integrals and Stochastic Processes," submitted to Physical Review A (1999).

[Ave99] D. V. Averin, "Solid State Qubits Under Control," Nature, Volume 398, 29th April (1999), pp748-749.

[Cer98] N. J. Cerf, L. K. Grover and C. P. Williams, "Nested Quantum Search for NP-Complete Problems," submitted to Physical Review A, (1998). Available as Los Alamos preprint http://xxx.lanl.gov/abs/quant-ph/9806078.

[Chu95] I. Chuang & Y. Yamamoto, "A Simple Quantum Computer", Los Alamos preprint archive, http://xxx.lanl.gov/archive/quant-ph/9505011, (1995)

[Chu98] I. L. Chuang, L. M. K. Vandersypen, X. Zhou, D. W. Leung, S. Lloyd, "Experimental realization of a quantum algorithm", Nature, 393, (1998) pp.143-146

[Cle97] R. Cleve, A. Ekert, C. Macchiavello, M. Mosca, "Quantum Algorithms Revisited," Proc. Roy. Soc. Lond. A (1997). Available as Los Alamos preprint http://xxx.lanl.gov/abs/quant-ph/9708016.

[DiV94] D. DiVincenzo and J. Smolin, "Results on two-bit gate design for quantum computers," in W. Porod and G. Frazier (eds.), Proceedings of the Second Workshop on Physics and Computation, PhysComp '94, IEEE Computer Society Press, pp.14-23. (1994)

[DiV96] D. DiVincenzo, "Topics in Quantum Computation," in "Mesoscopic Electron Transport", edited by L. Kowenhoven, G. Schoen and L. Sohn, NATO ASI Series E, Kluwer Ac. Publ., Dordrecht. (1996).

[Fij99] A. Fijany and C. P. Williams, "Quantum Wavelet Transforms: Fast Algorithms and Complete Circuits", in Springer-Verlag Lecture Notes in Computer Science, Volume 1509 (1999).

[Gin99] R. Gingrich, C. P. Williams, N. Cerf, "Generalized Quantum Search with Parallelism," http://xxx.lanl.gov/abs/quant-ph/9904049 (1999).

[Gro96] L. Grover, "A fast quantum mechanical algorithm for database search", Proceedings, 28th Annual ACM Symposium on the Theory of Computing (STOC), May (1996), pp.212-219

[Hog96] T. Hogg, ."Quantum Computing and Phase Transitions in Combinatorial Search," J. of Artificial Intelligence Research 4,91-128 (1996)

[Hog98] T. Hogg and M. Yanik, "Local Search Methods for Quantum Computers," http://xxx.lanl.gov/abs/quant-ph/9802043 (1998)

[Hog98] T. Hogg, C. Mochon, W. Polak, E. Rieffel,, "Tools for Quantum Algorithms," http://xxx.lanl.gov/abs/quant-ph/9811073 (1998)

[Hoy97] P. Hoyer, "Efficient Quantum Transforms," http://xxx.lanl.gov/abs/quant-ph/9702028 (1997)

[Iof99] L. B. Ioffe, V. B. Geshkenbein, M. V. Feigelman, A. L. Fauchere, and G. Blatter, "Environmentally Decoupled *sds*-Wave Josephson Junctions for Quantum Computing," Nature, Volume 398, 22nd April (1999), pp679-681.

[Jam98] D. F. V. James, M. S. Gulley, M. H. Holzscheiter, R. J. Hughes, P. G. Kwiat, S. K. Lamoreaux, C. G. Peterson, V. D. Sandberg, M. M. Schauer, C. M. Simmons, D. Tupa, P. Z. Wang, A. G. White, "Trapped Ion Quantum Computer Research at Los Alamos," Springer-Verlag Lecture Notes in Computer Science, Volume 1509, Springer-Verlag Heidelberg (1999).

[Jon98] J. A. Jones, M. Mosca, R. H. Hansen, "Implementation of a Quantum Search Algorithm on a Nuclear Magnetic Resonance Quantum Computer", Nature 393 (1998) pp.344-346

[Kan98] B. E. Kane, "A Silicon-Based Quantum Computer", Nature, Vol. 393 14th May (1998) pp. 133-137.

[Kaw99] R. K. Kawakami, E. Rotenberg, H. Choi, E. Escorcia-Aparicio, M. O. Bowen, J. H. Wolfe, E. Arenholz, Z. D. Zhang, N. V. smith and Z. Q. Qiu, "Quantum-Well States in Copper Thin Films," Nature, Volume 398, 11th March (1999), pp132-134.

[Llo93] S. Lloyd, "A Potentially Realizable Quantum Computer", Science, 261, (1993), pp.1569-1571.

[Mak99] Y. Makhlin, G. Schon, and A. Shnirman, "Josephson-Junction Qubits with Controlled Couplings," Nature, Volue 398, 25th March (1999), pp305-307.

[Nak99] Y. Nakamura, Y. A. Pashkin, and J. S. Tsai, "Coherent Control of Macroscopic quantum States in a Single Cooper-Pair Box," Nature, Volume 398, 29th April (1999), pp786-788.

[Pat98] R. Paturi, P. Pudlak, M. E. Saks, and F. Zane, "An Improved Exponential Time Algorithm for k-SAT," Proceedings of the 39th Annual Symposium on Foundations of Computer Science, FOCS'98, Palo Alto, November 8-11, IEEE Computer Society Press, Los Alamitos, CA (1998) pp628-637.

[Sel92] B. Selman, H. Levesque and D. Mitchell, "A New Method for Solving Hard Satisfiability Problems," in Proceedings of the Tenth National Conference on Artificial Intelligence, AAAI-92, San Jose, CA (1992) pp.440-446.

[Sch98] L. J. Schulman & U. Vazirani, "Scalable NMR Quantum Computation", Los Alamos preprint archive, http://xxx.lanl.gov/archive/quant-ph/9804060, (1998)

[Sel93] B. Selman, H. Kautz and B. Cohen, "Local Search Strategies for Satisfiability Testing," Proceedings of 2nd DIMACS Challenge on Cliques, Coloring and Satisfiability (1993)

[Sho94] P. Shor, "Algorithms for quantum computation: discrete logarithms and factoring", Proceedings 35th Annual Symposium on Foundations of Computer Science, Santa Fe, NM, USA, 20-22 Nov. 1994, IEEE Comput. Soc. Press (1994) pp. 124-134.

[Tuc99] R. Tucci, "A Rudimentary Quantum Compiler (2nd edition)," http://xxx.lanl.gov/abs/quant-ph/9902062 (1999)

[Wil98] C. P. Williams and S. H. Clearwater, "Explorations in Quantum Computing," TELOS/Springer-Verlag, ISBN 0-387-94768-X (1998).

[Wil99] C. P. Williams and A. Gray, "Automated Design of Quantum Circuits," in Springer-Verlag Lecture Notes in Computer Science, Volume 1509 (1999).